

**UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS
EASTERN DIVISION**

AMY GLAVIN, on behalf of herself and all
others similarly situated,

Plaintiff,

v.

CASNER & EDWARDS, LLP,

Defendant.

DEMAND FOR JURY TRIAL

Case No. _____

CLASS ACTION COMPLAINT

Amy Glavin (“Plaintiff”), through her attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Casner & Edwards, LLP (“Casner” or “Defendant”), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to her own actions, counsel’s investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendant’s failure to protect highly sensitive data.
2. Defendant is a Massachusetts-based law firm that offers legal services across a variety of practice areas.¹
3. As such, Defendant stores a litany of highly sensitive personal identifiable information (“PII”) about its current and former clients and opposing clients. But, between March

¹ About, Casner, <https://www.casneredwards.com/about/#content-block-two-section-stats> (last visited May 27, 2025).

21 and March 23, 2024, Defendant lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the “Data Breach”).²

4. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to the PII of least 12,979 of its current and former clients and opposing clients.³

5. On information and belief, cybercriminals were able to breach Defendant’s systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class’s PII. In short, Defendant’s failures placed the Class’s PII in a vulnerable position—rendering them easy targets for cybercriminals.

6. On or around May 20, 2025—more than *fourteen months* after the Data Breach first occurred—Casner finally began notifying Class Members about the Data Breach (“Breach Notice”). A copy of Plaintiff’s Breach Notice is attached as Exhibit A.

7. Plaintiff is a Data Breach victim. She brings this class action on behalf of herself, and all others harmed by Defendant’s misconduct.

8. The exposure of one’s PII to cybercriminals is a bell that cannot be unrung. Before this data breach, its current and former clients’ and opposing clients’ PII was exactly that—private. Not anymore. Now, their PII is forever exposed and unsecure.

PARTIES

9. Plaintiff, Amy Glavin, is a natural person and citizen of Massachusetts. She resides in Andover, Massachusetts where she intends to remain.

² Sample Breach Notice, Office of the Maine Attorney General, <https://www.maine.gov/cgi-bin/agviewerad/ret?loc=2602> (last visited May 27, 2025).

³ Breach Notification, Office of the Maine Attorney General, <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/368dac23-33bc-4f2b-b7a0-bd0e5012575f.html> (last visited May 27, 2025).

10. Defendant, Casner & Edwards, LLP, is a professional corporation formed under the laws of Massachusetts and with its principal place of business at 303 Congress St., 2nd Floor, Boston, MA 02210.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. There are over 100 putative Class Members.

12. This Court has personal jurisdiction over Defendant because it is headquartered in Massachusetts, and regularly conducts business in Massachusetts. Defendant and at least one member of the class are citizens of different states.

13. Venue is proper in this Court under because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

BACKGROUND

Defendant Collected and Stored the PII of Plaintiff and the Class

14. Defendant is a Massachusetts-based law firm that provides legal services across a range of practice areas. Defendant boasts that its clients “know the peace of mind that comes from partnering with a law firm whose experienced attorneys have one goal – doing what is best for the client.”⁴

15. As part of its business, Defendant receives and maintains the PII of its current and former clients and opposing clients.

⁴ Overview, LinkedIn, <https://www.linkedin.com/company/casner-&-edwards-llp/about/> (last visited May 27, 2025).

16. In collecting and maintaining the PII, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class members themselves took reasonable steps to secure their PII.

17. Under state and federal law, businesses like Defendant have duties to protect its current and former clients' and opposing clients' PII and to notify them about breaches.

18. Defendant recognizes these duties, declaring in its Breach Notice that "the confidentiality, privacy, and security of information in our care is one of our highest priorities." Ex. A.

Defendant's Data Breach

19. On or about April 10, 2024, Defendant "became aware of suspicious and unauthorized activity on [its] computer network initiated by persons outside of the Firm."⁵

20. Following the Data Breach, Defendant conducted an investigation that revealed that "an unknown actor gained access to certain parts of our network between March 21 and March 23, 2024."⁶

21. Worse, Defendant admitted that the cybercriminals "may have accessed or acquired certain files while on the network."⁷ Thus, on information and belief, Plaintiff's and Class Members' PII was stolen from Defendant's systems.

22. On or around May 20, 2025—more than *fourteen* months after the Data Breach first occurred—Casner finally began notifying Class Members about the Data Breach.

⁵ Sample Breach Notice, Office of the Maine Attorney General, <https://www.maine.gov/cgi-bin/agviewerad/ret?loc=2602> (last visited May 27, 2025).

⁶ *Id.*

⁷ *Id.*

23. Casner took over a year before informing Class Members even though Plaintiff and thousands of Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

24. Defendant's Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell its clients how the breach occurred and how many people were impacted.

25. Upon information and belief, the Breach impacted 12,979 individuals. And upon information and belief, this includes Defendant's current and former clients and opposing clients.

26. The Data Breach resulted in unauthorized disclosure, exfiltration, and theft of current and former clients' and opposing clients' highly personal information, including: name, Social Security number, financial account information, payment card information, and driver's license number.⁸

27. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII. And thus, Defendant caused widespread injury and monetary damages.

28. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

29. Because of Defendant's Data Breach, the sensitive PII of Plaintiff and Class members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class members.

⁸ *Id.*

30. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiffs' and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiffs' and the Class's financial accounts.

31. On information and belief, Defendant has offered 24 months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers. Ex. A.

32. Even with several months of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiffs' and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

33. Through its Breach Notice, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "protect against the possibility of the misuse of your information." Ex. A.

34. Additionally Defendant encouraged victims to "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."⁹

Plaintiff's Experiences and Injuries

35. Plaintiff Amy Glavin is a Data Breach victim, having received a Breach Notice in May 2025.

⁹ *Id.*

36. Plaintiff was the opposing party of one of Defendant's clients and her association with Defendant began in approximately 2017. Thus, Defendant obtained and maintained Plaintiff's PII. And as a result, Plaintiff was injured by Defendant's Data Breach.

37. Plaintiff (or her third-party agent) provided her PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

38. Upon information and belief, through its Data Breach, Defendant compromised Plaintiff's PII, including her name, Social Security number, financial account information, payment card information, and driver's license number. And upon information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

39. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach.

40. Plaintiff has and will spend considerable time and effort monitoring her accounts and researching the Data Breach to protect herself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach.

41. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

42. Plaintiff suffered actual injury from the exposure and theft of her PII—which violates her rights to privacy.

43. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

44. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant’s Data Breach placed Plaintiff’s PII right in the hands of criminals.

45. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries.

46. Today, Plaintiff has a continuing interest in ensuring that her PII—which, upon information and belief, remains backed up in Defendant’s possession—is protected and safeguarded from additional breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

47. Because of Defendant’s failure to prevent the Data Breach, Plaintiff and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

- a. loss of the opportunity to control how their PII is used;
- b. diminution in value of their PII;
- c. compromise and continuing publication of their PII;
- d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

- e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;
- f. delay in receipt of tax refund monies;
- g. unauthorized use of their stolen PII; and
- h. continued risk to their PII—which remains in Defendant’s possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII.

48. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to \$1,000.00 depending on the type of information obtained.

49. The value of Plaintiff and Class’s PII on the black market is considerable. Stolen PII trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the “Dark Web”—further exposing the information.

50. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII far and wide.

51. One way that criminals profit from stolen PII is by creating comprehensive dossiers on individuals called “Fullz” packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

52. The development of “Fullz” packages means that the PII exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet.

53. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and Class members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class members' stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

54. Defendant disclosed the PII of Plaintiff and Class members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and Class members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

55. Defendant's failure to promptly and properly notify Plaintiff and Class members of the Data Breach exacerbated Plaintiff and Class members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Consumers Prioritize Data Security

56. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."¹⁰ Therein, Cisco reported the following:

¹⁰ *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited March 19, 2025).

- a. “For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won’t purchase from an organization they don’t trust with their data.”¹¹
- b. “Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly.”¹²
- c. 89% of consumers stated that “I care about data privacy.”¹³
- d. 83% of consumers declared that “I am willing to spend time and money to protect data” and that “I expect to pay more” for privacy.¹⁴
- e. 51% of consumers revealed that “I have switched companies or providers over their data policies or data-sharing practices.”¹⁵
- f. 75% of consumers stated that “I will not purchase from organizations I don’t trust with my data.”¹⁶

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

¹¹ *Id.* at 3.

¹² *Id.*

¹³ *Id.* at 9.

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ *Id.* at 11.

57. Defendant’s data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

58. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.¹⁷

59. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, “[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”¹⁸

60. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant’s industry, including Defendant.

Defendant Failed to Follow FTC Guidelines

61. According to the Federal Trade Commission (“FTC”), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

¹⁷ See *2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) <https://notified.idtheftcenter.org/s/>.

¹⁸ Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware>.

62. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.¹⁹ The FTC declared that, *inter alia*, businesses must:

- a. protect the personal customer information that they keep;
- b. properly dispose of personal information that is no longer needed;
- c. encrypt information stored on computer networks;
- d. understand their network's vulnerabilities; and
- e. implement policies to correct security problems.

63. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

64. Furthermore, the FTC explains that companies must:

- a. not maintain information longer than is needed to authorize a transaction;
- b. limit access to sensitive data;
- c. require complex passwords to be used on networks;
- d. use industry-tested methods for security;
- e. monitor for suspicious activity on the network; and
- f. verify that third-party service providers use reasonable security measures.

65. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15

¹⁹ *Protecting Personal Information: A Guide for Business*, FED TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

66. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to its current and former clients' (and their current and former customers') data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

67. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

68. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

69. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04).

70. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

71. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

All individuals residing in the United States whose PII was compromised in the Casner & Edwards Data Breach, including all those individuals who received notice of the breach.

72. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

73. Plaintiff reserves the right to amend the class definition.

74. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

75. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them data breach notices.

76. Numerosity. The Class members are so numerous that joinder of all Class members is impracticable. Upon information and belief, the proposed Class includes at least 12,979 members.

77. Typicality. Plaintiff's claims are typical of Class members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

78. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. His interests do not conflict with Class members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

79. Commonality and Predominance. Plaintiff's and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class members—for which a class wide proceeding can answer for all Class members. In fact, a class wide proceeding is necessary to answer the following questions:

- a. if Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;
- b. if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. if Defendant were negligent in maintaining, protecting, and securing PII;
- d. if Defendant breached contract promises to safeguard Plaintiff and the Class's PII;
- e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;
- f. if Defendant's Breach Notice was reasonable;
- g. if the Data Breach caused Plaintiff and the Class injuries;

- h. what the proper damages measure is; and
- i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

80. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

81. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

82. Plaintiff and the Class (or their third-party agents) entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their PII, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

83. Defendant owed a duty of care to Plaintiff and Class members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry

standards for data security—would compromise their PII in a data breach. And here, that foreseeable danger came to pass.

84. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if their PII was wrongfully disclosed.

85. Defendant owed these duties to Plaintiff and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff and Class members' PII.

86. Defendant owed—to Plaintiff and Class members—at least the following duties to:

- a. exercise reasonable care in handling and using the PII in its care and custody;
- b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;
- c. promptly detect attempts at unauthorized access;
- d. notify Plaintiff and Class members within a reasonable timeframe of any breach to the security of their PII.

87. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

88. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain under applicable regulations.

89. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

90. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class (or their third-party agents) entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant.

91. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant hold vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII — whether by malware or otherwise.

92. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class members' and the importance of exercising reasonable care in handling it.

93. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

94. Defendant breached these duties as evidenced by the Data Breach.

95. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class members' PII by:

- a. disclosing and providing access to this information to third parties and

- b. failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

96. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and Class members which actually and proximately caused the Data Breach and Plaintiff and Class members' injury.

97. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class members' injuries-in-fact.

98. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

99. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

100. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

101. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted

from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

102. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

103. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff and Class members' PII.

104. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the Class members' sensitive PII.

105. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

106. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

107. The harm that has occurred is the type of harm the FTC Act are intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that,

because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

108. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

109. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

110. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

111. Had Plaintiff and members of the Class known that Defendant did not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

112. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

113. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their

PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their PII in its continued possession.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

114. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

115. Plaintiff and Class members either directly contracted with Defendant or Plaintiff and Class members were the third-party beneficiaries of contracts with Defendant.

116. Plaintiff and Class members (or their third-party agents) were required to provide their PII to Defendant as a condition of receiving services provided by Defendant. Plaintiff and Class members (or their third-party agents) provided their PII to Defendant in exchange for Defendant's services.

117. Plaintiff and Class members (or their third-party agents) reasonably understood that a portion of the funds they paid Defendant would be used to pay for adequate cybersecurity measures.

118. Plaintiff and Class members (or their third-party agents) reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

119. Plaintiff and the Class members (or their third-party agents) accepted Defendant's offers by disclosing their PII to Defendant or its third-party agents in exchange for services.

120. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII to unauthorized persons.

121. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiff's and Class Member's PII.

122. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class members (or their third-party agents) with prompt and adequate notice of all unauthorized access and/or theft of their PII.

123. After all, Plaintiff and Class members (or their third-party agents) would not have entrusted their PII to Defendant (or their third-party agents) in the absence of such an agreement with Defendant.

124. Plaintiff and the Class (or their third-party agents) fully performed their obligations under the implied contracts with Defendant.

125. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

126. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

127. Defendant materially breached the contracts it entered with Plaintiff and Class members (or their third-party agents) by:

- a. failing to safeguard their information;

- b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.
- c. failing to comply with industry standards;
- d. failing to comply with the legal obligations necessarily incorporated into the agreements; and
- e. failing to ensure the confidentiality and integrity of the electronic PII that Defendant created, received, maintained, and transmitted.

128. In these and other ways, Defendant violated its duty of good faith and fair dealing.

129. Defendant's material breaches were the direct and proximate cause of Plaintiff's and Class members' injuries (as detailed *supra*).

130. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

131. Plaintiff and Class members (or their third-party agents) performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

132. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

133. This claim is pleaded in the alternative to the breach of implied contract claim.

134. Plaintiff and Class members (or their third-party agents) conferred a benefit upon Defendant. After all, Defendant benefitted from (1) using their PII to facilitate its business, and (2) from accepting their payment.

135. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class members (or their third-party agents).

136. Plaintiff and Class members (or their third-party agents) reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

137. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' PII.

138. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

139. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class members' payment because Defendant failed to adequately protect their PII.

140. Plaintiff and Class members have no adequate remedy at law.

141. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class members—all unlawful or inequitable proceeds that it received because of its misconduct.

FIFTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

142. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

143. Given the relationship between Defendant and Plaintiff and Class members, where Defendant became guardian of Plaintiff's and Class members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class members,

(1) for the safeguarding of Plaintiff and Class members' PII; (2) to timely notify Plaintiff and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

144. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII.

145. Because of the highly sensitive nature of the PII, Plaintiff and Class members (or their third-party agents) would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

146. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' PII.

147. Defendant also breached its fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

148. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

PRAYER FOR RELIEF

Plaintiff and Class members respectfully request judgment against Defendant and that the Court enter an order:

- A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

- B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class;
- C. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the Class;
- D. Enjoining Defendant from further unfair and/or deceptive practices;
- E. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;
- F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;
- G. Awarding attorneys' fees and costs, as allowed by law;
- H. Awarding prejudgment and post-judgment interest, as provided by law;
- I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and
- J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Dated: June 2, 2025

By: /s/ Michael Appel
Michael Appel (BBO No. 543898)
Ketterer, Browne & Associates, LLC
336 S. Main Street
Bel Air, Maryland 21014
(617) 359-4981
Michael@KBAattorneys.com

Samuel J. Strauss (*Pro Hac Vice forthcoming*)
Raina C. Borrelli (*Pro Hac Vice forthcoming*)
STRAUSS BORRELLI PLLC
One Magnificent Mile

980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com

Attorneys for Plaintiff and the Proposed Class